Amendments to the Specification:

Please amend the specification as indicated below. Applicant avers that no new matter has been added. Added text is underlined and deleted text is either struck through or shown in double enclosing brackets. Amendments to the specification are made to better reflect terminology in the claims. The phrase "a whitelist" has been amended to recite "a recipient's whitelist" in claims 7, 8, 16, 17, 24, and 25 for better clarification and consistency. This is supported in the specification in paragraph [0023] by the phrase "[a] whitelist, created by the recipient." The phrase "a blacklist" has been appended to "a recipient's blacklist" in claims 8, 17, and 25 for better clarification and consistency. This is supported in the specification in paragraph [0025] by the phrase "a blacklist, created by the recipient."

Please amend Paragraph [0003] to replace the abbreviation "IP" with the text "Internet Protocol ('IP')" as shown below:

> [0003] It is possible to filter e-mail messages using software that is associated with a user's e-mail program. In addition to message text, e-mail messages contain a header having routing information (including [[IP]] Internet Protocol ("IP") addresses), a sender's address, recipient's address, and a subject line, among other things. The information in the message header may be used to filter messages. One approach is to filter e-mails based on words that appear in the subject line of the message. For instance, an e-mail user could specify that all e-mail messages containing the word "mortgage" be deleted or posted to a file. An e-mail user can also request that all messages from a certain domain be deleted or placed in a separate folder, or that only messages from specified senders be sent to the user's mailbox. These approaches have limited success since spammers frequently use subject lines that do not indicate the subject matter of the message (subject lines such as "Hi" or "Your request for information" are common). In addition, spammers are capable of forging addresses, so limiting e-mails based solely on domains or e-mail addresses might not result in a decrease of junk mail and might filter out e-mails of actual interest to the user.

Please amend Paragraph [0010] to replace the abbreviation "DNS" with the text "Domain Name System ('DNS')" as shown below:

> [0010] This need has been met by a method and software for processing e-mails and determining whether they are solicited or unsolicited by identifying information, based on data found either in the message or used in sending the message, about the origin of a received message (such as the sender and/or site), including at least one of: the actual sender; a final IP address; a final domain name; a normalized reverse [[DNS]] Domain Name System ("DNS") lookup of the final IP address; and an IP path used to send the message. Information about the origin of the message (as indicated by the identifying information discussed above) is collected and statistics about the origin of the message are compiled at at least one database and used to categorize whether the received message is solicited or unsolicited. These statistics are then used to determine whether or not the received message is spam.